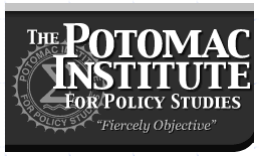
Homeland Security's Cyber Component: A Survey of Legal Issues

J. Bret Michael, Tom Wingfield
& Steve Roberts



Disclaimer

- The views and conclusions contained in this presentation are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the U.S. Government.

Five broad areas of legal issues

Legal preparedness

- "Legal preparation is a vital but often overlooked aspect … [and such preparedness] affords law enforcement the necessary powers to investigate and prosecute those who possess or attempt to use" weapons of mass destruction
  - R. Pagni, Consequence management in the 1995 sarin attacks on the Japanese subway system, *Studies in Conflict and Terrorism* 25, 6 (2002).

Example

- USA PATRIOT Act
  - Harmonizes and clarifies existing law regarding the interaction among
    - Law enforcement
    - Intelligence community
    - Military

Duty of care

- Provision of reasonable measures to mitigate terror vulnerabilities that might breach that duty, and thus create damages under contract, tort, and other corporate law
  - Legislation (California Act, HIPPA, GLB)
  - Case law (Remsburg *v*. DocuSearch)

Liability

- Safe harbors
  - Encryption under the California Security Breach Information Act
- New approaches to risk management
  - Cyber insurance
  - Terrorism Risk Insurance Act of 2002
  - Business continuity and planning

Use of force

- While fashioning responses to terrorist acts, law enforcement, military, and intelligence communities need to abide by
  - U.S. domestic law
  - Those portions of international law that the U.S. recognizes
- What constitutes a use of force or armed aggression under international law?
- How does traditional law of conflict apply to operations in cyberspace?

Examples

- UN Charter defines armed aggression in terms of kinetic warfare
  - Schmitt Analysis can be used to reduce the "gray cloud of uncertainty," looking at effect rather than solely the means of attack
- How does one apply the customary rules of war in information conflict?
  - Discrimination, necessity, proportionality and chivalry

Military/Intelligence

- To what extent should the US military be involved in conducting domestic counterterrorism operations? (Posse Commitatus)
- To what extent may the intelligence community share information on US persons? (intelligence oversight)

Information sharing

- Voluntary (bottom-up)
  - Example: AGORA
- Legislated (top-down)
  - Example: Homeland Security Act of 2002 provides encouragement for the private sector to participate in Information Sharing and Analysis Centers (ISACs) and other information-sharing arrangements

Example of information sharing

- Data Retention
  - Collect all intercepted communication data or content
  - Can be made voluntary or mandatory
  - Can be instituted by both
    - Governments
    - Non-governmental organizations (NGOs)
- Data Preservation
  - Does not treat the collection of data
  - Preserve existing data of a specific
    - Type
    - Person or group
    - Time period
  - Typically conducted on a case-by-case basis via a court order

Some legal issues related to retention and preservation

- Use of communication data, for instance, for predictive purposes - need special controls?
- There are different legal regimes in place for governing communication data and content
- There is little customary international law on data retention